

FORM PTO-1390 (REV 12-29-99)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY'S DOCKET NUMBER 82032-0003
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371			
INTERNATIONAL APPLICATION NO.		INTERNATIONAL FILING DATE	
PCT/EP99/00283		14 January 1999 (14.01.99)	
PRIORITY DATE CLAIMED			
14 January 1998 (14.01.98)			
TITLE OF INVENTION			
METHOD FOR TRANSFERRING DATA FROM A HEAD-END TO A NUMBER OF RECEIVERS			
APPLICANT(S) FOR DO/EO/US			
Andrew Augustine WAJS			
<p>Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:</p> <ol style="list-style-type: none"> <li><input checked="" type="checkbox"/> This is a <b>FIRST</b> submission of items concerning a filing under 35 U.S.C. 371.</li> <li><input type="checkbox"/> This is a <b>SECOND</b> or <b>SUBSEQUENT</b> submission of items concerning a filing under 35 U.S.C. 371.</li> <li><input checked="" type="checkbox"/> This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).</li> <li><input checked="" type="checkbox"/> A proper Demand for International Preliminary Examination was made by the 19<sup>th</sup> month from the earliest claimed priority date.</li> <li><input checked="" type="checkbox"/> A copy of the International Application as filed (35 U.S.C. 371(c)(2))             <ol style="list-style-type: none"> <li><input type="checkbox"/> is transmitted herewith (required only if not transmitted by the International Bureau).</li> <li><input checked="" type="checkbox"/> has been transmitted by the International Bureau.</li> <li><input type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US).</li> </ol> </li> <li><input type="checkbox"/> A translation of the International Application into English (35 U.S.C. 371(c)(2)).</li> <li><input type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))             <ol style="list-style-type: none"> <li><input type="checkbox"/> are transmitted herewith (required only if not transmitted by the International Bureau).</li> <li><input type="checkbox"/> have been transmitted by the International Bureau.</li> <li><input type="checkbox"/> have not been made; however, the time limit for making such amendments has NOT expired.</li> <li><input type="checkbox"/> have not been made and will not be made.</li> </ol> </li> <li><input type="checkbox"/> A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).</li> <li><input type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).</li> <li><input type="checkbox"/> A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).</li> </ol> <p>Items 11. to 16. below concern document(s) or information included:</p> <ol style="list-style-type: none"> <li><input type="checkbox"/> An Information Disclosure Statement under 37 CFR 1.97 and 1.98.</li> <li><input type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.</li> <li><input checked="" type="checkbox"/> A <b>FIRST</b> preliminary amendment.             <ol style="list-style-type: none"> <li><input type="checkbox"/> A <b>SECOND</b> or <b>SUBSEQUENT</b> preliminary amendment.</li> </ol> </li> <li><input type="checkbox"/> A substitute specification.</li> <li><input type="checkbox"/> A change of power of attorney and/or address letter.</li> <li><input checked="" type="checkbox"/> Other items or information:             <ul style="list-style-type: none"> <li>-Courtesy copy of the International Application as published with International Search Report.</li> <li>-Courtesy copy of the International Preliminary Examination Report as published.</li> </ul> </li> </ol>			

U.S. APPLICATION NO. (or Patent No. 70111.5)	INTERNATIONAL APPLICATION NO. PCT/EP99/00283	ATTORNEY'S DOCKET NUMBER 82032-00003
<input checked="" type="checkbox"/> The following fees are submitted: <b>BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5):</b> <ul style="list-style-type: none"> <li>Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO ..... <b>\$970.00</b></li> <li>International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO ..... <b>\$840.00</b></li> <li>International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO ..... <b>\$690.00</b></li> <li>International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy Provisions of PCT Article 33(1)-(4) ..... <b>\$670.00</b></li> <li>International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) ..... <b>\$96.00</b></li> </ul>		<b>CALCULATIONS PTO USE ONLY</b>
<b>ENTER APPROPRIATE BASIC FEE AMOUNT =</b>		\$840.00
Surcharge of <b>\$130.00</b> for furnishing the oath or declaration later than <input type="checkbox"/> 20 X 30 months from the earliest claimed priority date (37 CFR 1.492(e)).		130 (not included) \$
CLAIMS	NUMBER FILED	NUMBER EXTRA
Total claims	5-20 =	X \$18.00
Independent claims	1- 3 =	X \$78.00
MULTIPLE DEPENDENT CLAIM(S) (if applicable)		+\$260.00
<b>TOTAL OF ABOVE CALCULATIONS =</b>		\$840.00
Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28).		
<b>SUBTOTAL =</b>		\$840.00
Processing fee of <b>\$130.00</b> for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)).		+
<b>TOTAL NATIONAL FEE =</b>		\$840.00
Fee for recording the enclosed assignment (37 CFR 1.21(b)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). <b>\$40.00</b> per property		+
<b>TOTAL FEES ENCLOSED =</b>		\$840.00
		Amount to be refunded: charged: <b>\$</b>
<p>a. <input checked="" type="checkbox"/> A check in the amount of <b>\$ 840.00</b> to cover the above fees is enclosed.</p> <p>b. <input type="checkbox"/> Please charge my Deposit Account No. _____ in the amount of <b>\$</b> _____ to cover the above fees. A duplicate copy of this sheet is enclosed.</p> <p>c. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-1349. A duplicate copy of this sheet is enclosed.</p>		
<p><b>NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.</b></p> <p>SEND ALL CORRESPONDENCE TO:  <b>HOGAN &amp; HARTSON LLP</b>  Celine Jimenez Crowsen  555-13<sup>th</sup> Street, N.W., 7W  Washington, D.C. 20004  (202) 637-5703</p>		
 <p>SIGNATURE  <b>CELINE JIMENEZ CROWSEN</b>  NAME  40-357  REGISTRATION NUMBER</p>		

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: ) 354 REC & PCT/PCT 12 JUL 2000  
 )  
 Andrew A. WAJS ) 371 of International Application  
 )  
 Serial No.: not yet assigned ) IA #: PCT/EP99/00283  
 )  
 Filed: even date herewith ) IA Date: 14 January 99  
 )  
 Title: METHOD FOR TRANSFERRING )  
 DATA FROM A HEAD-END )  
 TO A NUMBER OF RECEIVERS ) ATTY DKT NO.: 82032-00003

## PRELIMINARY AMENDMENT

Commissioner of Patents and Trademarks  
Washington, D.C.

Sir:

Prior to calculation of the filing fee and examination on the merits, please amend the above-identified application as follows:

**IN THE CLAIMS:**

Claim 3, line 1, delete "or 2".  
Claim 4, line 1, delete "2 or 3.".   
Claim 5, lines 1 and 2, change "any one of the preceding claims" to  
--claim 1--

## REMARKS

The above amendments are being made to delete multiple dependencies in the claims and does not add to or depart from the original disclosure or constitute prohibited new matter.

Respectfully submitted,

Celine Jimenez Crowson  
Attorney for Applicant  
Hogan & Hartson, LLP  
555 13<sup>th</sup> Street, N.W., Suite 701-W  
Washington, D.C. 20004  
PH: 202-637-5600

Method for transferring data from a head-end to a number of receivers

The present invention relates to a method for transferring data from a head-end to a number of receivers by means of a digital broadcast signal, each of said receivers including a descrambler for descrambling a received digital transport stream.

The use of a digital broadcast signal, such as a DVB signal, for transferring data to one or more receivers shows the advantage that available receivers with descramblers can be used to transfer the data from a head-end to the receiver. However, such a method would normally not allow for a data transfer in a secure and private manner as the data is accessible to all receivers listening to the digital transport stream.

The present invention aims to provide a method of the above-mentioned type wherein privacy and security of the data transfer can be provided to each receiver.

According to the invention a method of the above-mentioned type is provided, including sending a message from the head-end to each receiver to which data needs to be transferred, said message including a key unique to the respective receiver, loading the unique key in the descrambler of the respective receiver, providing a table of unique keys with corresponding addresses of the respective receivers at the head-end, providing data packets with an individual address of at least one of said receivers, inserting said data packets into transport packets of a digital transport stream, selecting a key from said table in accordance with the address of the data packets, scrambling

5 said transport packets using the selected key, broadcasting the digital transport stream, receiving the digital transport stream at one or more receivers and descrambling the scrambled transport packets of the digital transport stream only at the receiver having the unique key used to scramble the scrambled transport packets.

In this manner a method is obtained wherein each receiver attempting to descramble the broadcast signal will fail to descramble the signal accept for the receiver(s) 10 having the unique key(s) used to scramble the transport packets in which the data packets are inserted which are intended to be received by this receiver. This results in the desired privacy and security for the data transfer between the head-end and the receiver.

15 In a preferred embodiment for transferring data packets to two or more receivers, the data packets for different receivers are inserted into different transport packets, each of said transport packets being scrambled with a unique key corresponding with the individual address of the 20 corresponding data packets.

In this manner data transfer with privacy and security is provided for a number of receivers requesting the transfer of data.

The invention will be further explained by reference 25 to the drawings in which an embodiment of the invention is schematically shown.

In this preferred embodiment the method is used to transfer data requested by a receiver from the Internet to the receiver on a digital broadcast signal or digital 30 transport stream, so that an Internet connection is obtained with a high speed transfer of data to the receiver according to the Internet Protocol. However the method described can

also be used to transfer data to receivers at their request or initiated by the head-end in another manner.

In the drawing a DVB system is very schematically shown by way of example, the system comprising head-end equipment 1 which will be indicated hereinafter by head-end, and a large number of subscribers having a receiver 2, only one of which is shown in the drawing. The receiver 2 includes a descrambler 3 co-operating with a smart card 4 in a usual manner. The descrambler 3 is used to descramble DVB services requiring a subscription. The receiver 2 is connected to the Internet 5 in a manner not further shown, for example by a well-known modem. If the receiver 2 requests the download of data, the data will be transferred to the receiver 2 via the head-end 1 by means of a broadcast signal in the following manner.

According to the internet protocol the data includes an IP or MAC address of the receiver 2 requesting the data to be transferred to this receiver. Each receiver 2 for which the head-end 1 receives data packets with an individual address, i.e. the IP or MAC address, is sent a so-called Entitlement Control Message or ECM with a control word or key which is unique to the receiver 2. This message is encrypted using an individual key which is stored in the smart card 4. At the head-end 1 the unique keys with the corresponding individual addresses are stored in a table 6. At the receiver(s) 2 to which an ECM is sent, the smart card 4 decrypts the received message using its individual key to obtain the unique key. The decrypted key is loaded into the descrambler 3 for future use.

At the head-end 1, the data packets for a specific receiver 2 requesting the transfer of data, are inserted into transport packets of the digital transport stream. Generally, the data packets are larger than the transport stream

packets, so that the data packets are split and thereafter inserted into a number of transport stream packets. Before scrambling the transport stream packets containing the data packets, the head-end checks the IP or MAC address and 5 selects the corresponding unique key from the table 6, which key is used to scramble the transport stream packets.

Each receiver 2 listening to the digital broadcast signal attempts to descramble the transport stream packets of the digital transport stream, wherein however only at the 10 receiver 2 having the unique key used for scrambling the transport stream packets, the descrambling process will be successful. In this manner only one receiver 2 will descramble the scrambled transport stream packets to thereby obtain the IP data packets.

15 From the above it will be clear that the described method results in a transfer of data with privacy and security for each receiver 2 requesting a data transfer. Moreover, this transfer with privacy and security is achieved while using existing DVB or MPEG scrambling and descrambling 20 equipment.

Generally, a number of receivers 2 will request the transfer of data. This is no problem as the head-end 1 will provide a table 6 including key/address combinations for each receiver 2 requesting a data transfer. The capacity of a 25 digital broadcast signal is sufficient to transfer IP data packets to a large number of receivers 2. As the IP data packets for each particular receiver will be inserted into a number of transport packets wherein only these transport packets are scrambled using the unique key for this particular receiver, data transfer will still take place in a 30 private and secure manner.

The data packets can be inserted into transport stream packets of a digital transport stream which is used

for the transfer of data only. As an alternative the data packets can be inserted into transport stream packets of a DVB transport stream as the capacity of such a transport stream is far more than necessary for transferring the video information.

Although in the preferred embodiment the method is used to transfer IP data packets, the described method can also be used to transfer data from other sources than the Internet. Further, it is noted that instead of an ECM another type of message may be used to transfer a unique key to a receiver.

CLAIMS

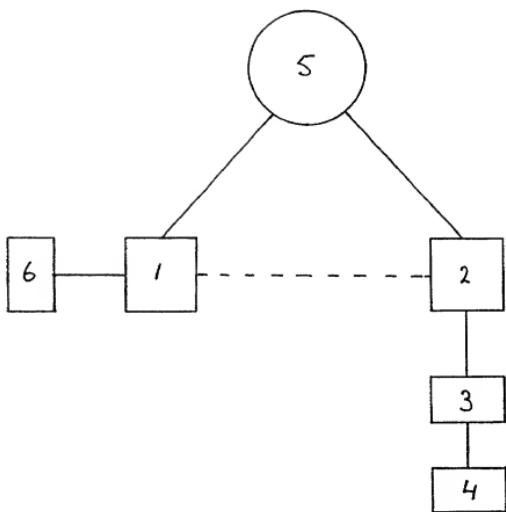
1. Method for transferring data from a head-end to a number of receivers by means of a digital broadcast signal, each of said receivers including a descrambler for descrambling a received digital transport stream, said method 5 including sending a message from the head-end to each receiver to which data needs to be transferred, said message including a key unique to the respective receiver, loading the unique key in the descrambler of the respective receiver, providing a table of unique keys with corresponding addresses 10 of the respective receivers at the head-end, providing data packets with an individual address of at least one of said receivers, inserting said data packets into transport packets of a digital transport stream, selecting a key from said table in accordance with the address of the data packets, 15 scrambling said transport packets using the selected key, broadcasting the digital transport stream, receiving the digital transport stream at one or more receivers and descrambling the scrambled transport packets of the digital transport stream only at the receiver having the unique key 20 used to scramble the scrambled transport packets.

2. Method according to claim 1, wherein for transferring data packets to two or more receivers, the data packets for different receivers are inserted into different transport packets, each of said transport packets being 25 scrambled with a unique key corresponding with the individual address of the corresponding data packets.

3. Method according to claim 1 or 2, wherein each receiver is adapted to request the transfer of specific data from the head-end.

4. Method according to claim 1, 2 or 3, wherein  
5 the head-end and the receivers are connected to a network, for example the internet, wherein one or more receivers request the transfer of data from the network, wherein the requested data together with the address of the requesting receiver(s) is provided to the head-end in the form of data  
10 packets and the head-end transfers the data packets to said one or more receivers inserted in transport packets of the digital broadcast stream.

5. Method according to any one of the preceding claims, wherein the digital transport stream is a DVB  
15 transport stream.



**Declaration and Power of Attorney for Patent Application**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought, on the invention entitled **METHOD FOR TRANSFERRING DATA FROM HEAD-END TO A NUMBER OF RECEIVERS**, the specification of which

is attached hereto.

was filed on July 12, 2000  
Application Serial No. 09/600,121  
and was amended on \_\_\_\_\_

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

		Priority Claimed		
<u>98200081.2</u>	<u>EP</u>	<u>14/JANUARY/1998</u>	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
(Number)	(Country)	(Day/Month/Year)		

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

(Application Serial No.) (Filing Date)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

PCT/EP99/00283 14JANUARY1999 (Status)

(Application Serial No.) (Filing Date) (Status)

I or we hereby appoint the following attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith, and request that all correspondence about the application be addressed to HOGAN & HARTSON L.L.P., 555 13th Street, N.W., Washington, D.C. 20004

 Celine Jimenez Crowson, Reg. No. 40,357  
 Kevin G. Shaw, Reg. No. 43,110

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

FIRST NAMED INVENTOR	SIGNATURE	DATE
Andrew Augustine WAJS		08/09/00
RESIDENCE	CITIZENSHIP	
NL-2023 AA Haarlem	Great Britain/Netherlands	
POST OFFICE ADDRESS		
Schotersingel 93, NL-2023 AA Haarlem, The Netherlands		